POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

UNIFESSPA
Universidade Federal do Sul e Sudeste do Pará

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
13/12/2017	1.0	Publicação da POSIC	Fernando Alves Miranda
21/07/2020	1.1	Adequação à EGD 2020-2022	Ralfh Alan Gomes Machado

SUMÁRIO

1. ESCOPO

1.1. A Política de Segurança da Informação e Comunicação - PoSIC da Universidade Federal do Sul e Sudeste do Pará – Unifesspa tem como principal objetivo garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas e custodiadas pela Instituição

1.2. São partes integrantes desta PoSIC os principais procedimentos e normas complementares destinados ao resguardo da informação e à disciplina na sua utilização.

1.3. As diretrizes de Segurança da Informação e Comunicações - SIC devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura da Unifesspa.

1.4. A Gestão de Segurança da Informação e Comunicações - GSIC deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SIC.

1.5. As instruções, normas complementares e manuais de procedimentos da PoSIC da Unifesspa aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, bolsistas de iniciação científica, consultores externos e a quem, de alguma forma, executem atividades vinculadas a esta Instituição de Ensino Superior - IFES.

1.6. Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicações.

1.7. Todos os contratos, convênios, acordos e outros instrumentos semelhantes celebrados por esta IFES devem atender a esta PoSIC.

1.8. Esta política também se aplica, no que couber, ao relacionamento da Unifesspa com terceiros.

2. CONCEITOS E DEFINIÇÕES

No âmbito da PoSIC considera-se:

2.1. **Agente responsável que compõe a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR**: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal incumbido de chefiar e gerenciar a ETIR;

2.2. **Ameaça**: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

2.3. **Ativos de informação**: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

2.4. **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

2.5. **Capacitação em SIC**: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;

2.6. **Classificação da informação**: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

2.7. **Comitê de Governança Digital - CGD**: colegiado de caráter deliberativo também responsável pela normatização e supervisão da segurança da informação e comunicações no âmbito da Unifesspa;

2.8. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

2.9. **Conscientização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

2.10. **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

2.11. **CTIR.GOV**: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República DSIC/GSI/PR;

2.12. **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

2.13. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;

2.14. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR**: colegiado composto por servidores públicos ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do Unifesspa;

2.15. **Especialização em SIC**: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na organização como gestor de SIC e tornando-se referência na pesquisa de novas soluções e modelos de SIC;

2.16. **Estrutura de GSIC**: grupo responsável pela gestão e execução da SIC;

2.17. **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

2.18. **Gestão de continuidade dos negócios**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

2.19. **Gerenciamento de operações e comunicações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;

2.20. **Gestão de riscos de segurança da informação e comunicações - GRSIC**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;

2.21. **Gestão de segurança da informação e comunicações - GSIC**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;

2.22. **Gestor dos ativos de informação**: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

2.23. **Gestor de SIC**: servidor nomeado pelo Reitor da Unifesspa como responsável pela gestão de segurança da informação e comunicações no âmbito do órgão e pela coordenação da ETIR;

2.24. **Incidente de SIC**: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

2.25. **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

2.26. **Infraestrutura de TI**: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

2.27. **Integridade**: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental;

2.28. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

2.29. **Recursos criptográficos**: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

2.30. **Risco de SIC**: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

2.31. **Segurança física e do ambiente**: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

2.32. **Sensibilização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional;

2.33. **Sistema estruturante**: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

2.34. **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao Unifesspa;

2.35. **Tratamento de incidentes**: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

2.36. **Tratamento da informação**: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação; e

2.37. **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3. PRINCÍPIOS

3.1. A PoSIC deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

3.2. A PoSIC deve orientar-se pelos seguintes princípios da SIC: confidencialidade, integridade, disponibilidade e autenticidade.

4. DIRETRIZES GERAIS

4.1. Deverá haver avaliação periódica do cumprimento desta política de segurança e de suas normas complementares através de análises de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Governança Digital – CGD.

4.2. Fica instituída a Estrutura de GSIC da Unifesspa, composta pelo Comitê de Governança Digital - CGD e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, os quais serão solidariamente responsáveis pelas seguintes atividades:

a) executar os processos de segurança da informação e comunicações;

b) desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos da Unifesspa;

c) avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação e desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;

d) fornecer subsídios visando à verificação de conformidade de segurança da informação e comunicações; e

e) promover a melhoria contínua nos processos e controles de GSIC.

f) instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em SIC, buscando parcerias com outros órgãos e entidades

4.3. A Estrutura de GSIC deve definir um Plano de SIC para a Unifesspa.

4.4. A Estrutura de GSIC da Unifesspa deve possuir um sistema de registro de incidentes de SIC.

4.5. Os membros da Estrutura da GSIC devem receber regularmente capacitação especializada nas disciplinas relacionadas à SIC de acordo com suas funções.

4.6. A GSIC da Unifesspa deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da instituição e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

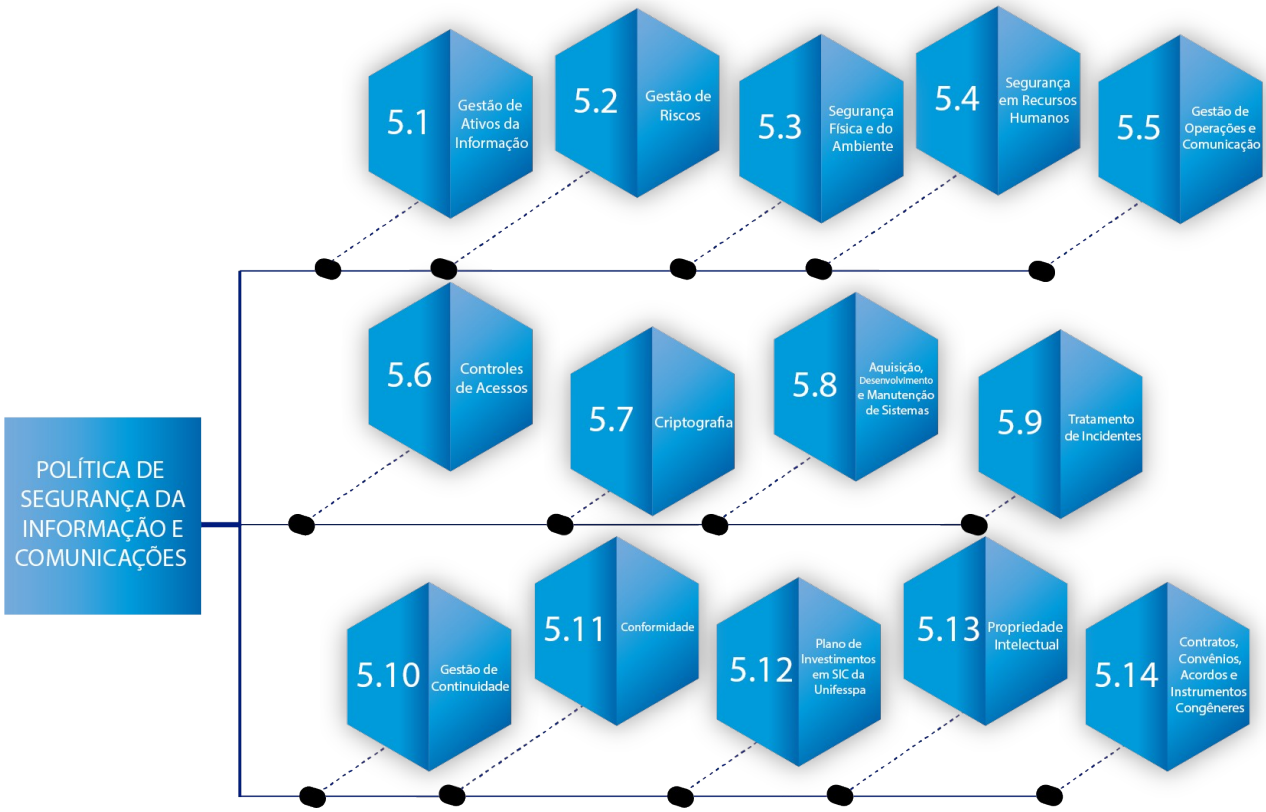
4.7. A Estrutura de GSIC deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

4.8. A Unifesspa, além das diretrizes estabelecidas nesta PoSIC, deve também se orientar pelas melhores práticas e procedimentos de SIC recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

4.9. É vetado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela Unifesspa.

4.10. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

4.11. Os contratos firmados pela Unifesspa devem conter cláusulas que determinem a observância da PoSIC e seus respectivos documentos.



5. DIRETRIZES ESPECÍFICAS

Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaborados normas táticas específicas, manuais e procedimentos.

5.1 Gestão de Ativos da Informação

5.1.1. Os ativos de informação devem:

a) ser inventariados e protegidos;

b) ter identificados os seus proprietários e custodiantes;

c) ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

d) ter a sua entrada e saída nas dependências da Unifesspa autorizadas e registradas por autoridade competente;

e) ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

f) ser regulamentados por norma específica quanto a sua utilização; e

g) ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

5.1.2. A Unifesspa deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

5.1.3. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

5.1.4. Os sistemas de informação e as aplicações da Unifesspa devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

5.1.5. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

5.2 Gestão de Riscos

5.2.1. O gestor dos ativos de informação deve estabelecer processos de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.

5.2.2. A GRSIC é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações, levando em consideração o planejamento, execução, análise crítica e melhoria da SIC na Unifesspa.

5.3. Segurança Física e do Ambiente

5.3.1. A Estrutura de GSIC deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

5.3.2. As proteções devem estar alinhadas aos riscos identificados.

5.4. Segurança em Recursos Humanos

5.4.1. Os usuários devem ter ciência:

a) das ameaças e preocupações relativas à SIC; e

b) de suas responsabilidades e obrigações no âmbito desta PoSIC.

5.4.2.Todos os usuários devem difundir e exigir o cumprimento da PoSIC, das normas de segurança e da legislação vigente acerca do tema.

5.4.3. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários da Unifesspa, de acordo com suas competências funcionais.

5.4.4. Os usuários devem ser sensibilizados e conscientizados para apoiar esta PoSIC durante os seus trabalhos normais.

5.4.5. Em relação ao controle de pessoal deve estabelecer controles de perfis, permissões e procedimentos necessários para a salvaguarda da SIC.

5.5. Gestão de Operações e Comunicação

A Estrutura de GSIC deve estabelecer parâmetros adequados, relacionados à SIC, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da Unifesspa. Os acordos de nível de serviço devem ser compatíveis com padrões de mercado e requisitos de segurança.

5.6. Controles de Acessos

5.6.1. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

5.6.2. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

5.6.3. Os usuários da Unifesspa são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.

5.6.4. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

5.6.5. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e

qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.

5.6.6. Todos os sistemas de informação da Unifesspa, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

5.6.7. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento da Unifesspa ou bloqueados em caso de afastamento.

5.6.8. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:

a) ao acesso às suas bases de dados;

b) à extração, carga e transformação de dados; e

c) aos serviços acessíveis via linguagem de programação.

5.6.9. Os sistemas estruturantes devem possuir mecanismos automáticos para:

a) revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;

b) bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor; e

c) tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

5.7. Criptografia

5.7.1. O uso de recursos criptográficos interfere na DICA, sendo, portanto, responsabilidade do Gestor de SIC a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas na Unifesspa, em conformidade com as orientações contidas em norma específica.

5.7.2. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

5.8. Aquisição, Desenvolvimento e Manutenção de Sistemas

5.8.1. A Estrutura de GSIC deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

5.8.2. O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

5.9. Tratamento de Incidentes

5.9.1. A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo do CTIR.GOV.

5.9.2. Deve ser instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança.

5.10. Gestão de Continuidade

A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam a Gestão de Continuidade do Negócio.

5.11. Conformidade

5.11.1. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC da Unifesspa e de suas unidades administrativas com esta PoSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC.

5.11.2. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a Unifesspa.

5.11.3. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de CGD e aprovado pelo CGD.

5.11.4. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

5.11.5. Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SIC por período superior a 2 (dois) anos.

5.11.6. A execução da verificação de conformidade será realizada pela Estrutura de GSIC, podendo, com a prévia aprovação do CGD, ser subcontratada no todo ou em parte.

5.11.7. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

5.11.8. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (*logs*), análise de código-fonte, entrevistas e testes de invasão.

5.11.9. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de SIC ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

5.12. Plano de Investimentos em SIC da Unifesspa

5.12.1. Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos.

5.12.2. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

5.12.3. O plano de investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo CGD, mediante recomendação elaborada pela Estrutura de GSIC.

5.12.4. Caso haja limitação na execução orçamentária, caberá ao CGD realizar a correspondente revisão do plano de investimentos.

5.13. Propriedade Intelectual

5.13.1. As informações produzidas por usuários no exercício de suas funções, são patrimônio intelectual da Unifesspa e não cabe a seus criadores qualquer forma de direito autoral.

5.13.2. É vedada a utilização de informações produzidas por terceiros para uso exclusivo da Unifesspa em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Presidente, nos demais casos.

5.14. Contratos, Convênios, Acordos e Instrumentos congêneres

5.14.1. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

5.14.2. Os acordos com terceiros podem também envolver outras partes.

5.14.2.1. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pela Unifesspa.

5.14.3. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC e de suas normas complementares.

5.14.4. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na Unifesspa.

5.14.5. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

5.14.6. Deve ser definido um processo adequado/objetivo de gestão de mudanças que será detalhado em norma específica.

6. PENALIDADES

Ações que violem a PoSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1. Cabe ao Gestor de SIC:

a) promover cultura de segurança da informação e comunicações;

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor recursos necessários às ações de SIC;

d) coordenar a ETIR;

e) comunicar ao CGD os resultados e outras informações pertinentes;

f) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

g) propor normas relativas à SIC.

7.2. Cabe ao CGD:

a) normatizar e supervisionar a SIC no âmbito da Unifesspa;

b) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

c) propor alterações na PoSIC;

d) solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

e) avaliar, revisar e analisar criticamente a PoSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais da Unifesspa e às legislações vigentes;

f) dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIC da Unifesspa;

g) constituir grupo de trabalho para realizar verificações de conformidade;

h) aprovar o plano de investimentos em SIC da Unifesspa;

i) monitorar e avaliar periodicamente o plano de SIC, assim como determinar os ajustes cabíveis;

j) definir e atualizar seu Regimento Interno; e

k) baixar normas e procedimentos complementares a esta PoSIC.

7.3. Cabe à ETIR:

a) facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

b) promover a recuperação de sistemas;

c) agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

d) realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

e) analisar ataques e intrusões na rede da Unifesspa;

f) executar as ações necessárias para tratar quebras de segurança;

g) obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

h) cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

i) participar em fóruns, redes nacionais e internacionais relativos à SIC.

7.4. Cabe ao Gestor do Ativo de Informação:

a) garantir a segurança dos ativos de informação sob sua responsabilidade;

b) definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PoSIC;

c) conceder e revogar acessos aos ativos de informação;

d) comunicar à ETIR a ocorrência de incidentes de SIC; e

e) designar custodiante dos ativos de informação, quando aplicável.

7.5. Cabe ao custodiante do ativo de informação

Proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PoSIC.

7.6. Cabe ao titular da unidade administrativa:

a) corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;

b) conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

c) incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

d) tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

e) realizar o tratamento e a classificação da informação;

f) autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

g) comunicar à ETIR os casos de quebra de segurança; e

h) manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

7.7. Cabe aos terceiros e fornecedores, conforme previsto em contrato:

a) tomar conhecimento desta PoSIC;

b) fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

c) fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

7.8. Cabe aos usuários:

a) conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PoSIC, bem como os demais normativos e resoluções relacionados à SIC;

b) obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

c) comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à ETIR.

8. ALINHAMENTO ESTRATÉGICO

Alinhar os recursos organizacionais com as estratégias da Instituição.

8.1. Promover Segurança da Informação e Comunicação na Unifesspa (OE.03).

8.2. Promover a disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação custodiados pela Unifesspa.

8.3. Promover proteção da informação pessoal e de propriedade intelectual.

8.1 ESTRATÉGIA DO GOVERNO DIGITAL (EGD)

Os objetivos estratégicos de TIC da Unifesspa foram baseados na Estratégia de Governo Digital 2020-2022. A Estratégia de Governo Digital para o período de 2020 a 2022 está organizada em princípios, objetivos e iniciativas que nortearão a transformação do governo por meio do uso de tecnologias digitais, com a promoção da efetividade das políticas e da qualidade dos serviços públicos e com o objetivo final de reconquistar a confiança dos brasileiros. O quadro abaixo lista estes objetivos:

Quadro 1: objetivos estratégicos (EGD)

ID	Objetivos Estratégicos
OE.EGD.01	Oferta de serviços públicos digitais
OE.EGD.02	Avaliação de satisfação nos serviços digitais
OE.EGD.03	Canais e serviços digitais simples e intuitivos
OE.EGD.04	Acesso digital único aos serviços públicos
OE.EGD.05	Plataformas e ferramentas compartilhadas
OE.EGD.06	Serviços públicos integrados
OE.EGD.07	Políticas públicas baseadas em dados e evidências
OE.EGD.08	Serviços públicos do futuro e tecnologias emergentes

OE.EGD.09	Serviços preditivos e personalizados ao cidadão
OE.EGD.10	Implementação da Lei Geral de Proteção de Dados no âmbito do Governo federal
OE.EGD.11	Garantia da segurança das plataformas de governo digital e de missão crítica
OE.EGD.12	Identidade digital ao cidadão
OE.EGD.13	Reformulação dos canais de transparência e dados abertos
OE.EGD.14	Participação do cidadão na elaboração de políticas públicas
OE.EGD.15	Governo como plataforma para novos negócios
OE.EGD.16	Otimização das infraestruturas de tecnologia da informação
OE.EGD.17	O digital como fonte de recursos para políticas públicas essenciais
OE.EGD.18	Equipes de governo com competências digitais

O decreto Nº 10.332, de 28 de abril de 2020, instituiu a EGD e detalhou seus objetivos:

- **Objetivo 1 - Oferta de serviços públicos digitais**

  Iniciativa 1.1. Transformar todas as etapas e os serviços públicos digitalizáveis, até 2022;

  Iniciativa 1.2. Simplificar e agilizar a abertura, a alteração e a extinção de empresas no Brasil, de forma que esses procedimentos possam ser realizados em um dia, até 2022.

- **Objetivo 2 - Avaliação de satisfação nos serviços digitais**

  Iniciativa 2.1. Oferecer meio de avaliação de satisfação padronizado para, no mínimo, cinquenta por cento dos serviços públicos digitais, até 2022;

  Iniciativa 2.2. Aprimorar a satisfação dos usuários dos serviços públicos e obter nível médio de, no mínimo, 4,5 (quatro inteiros e cinco décimos) em escala de 5 (cinco) pontos, até 2022;

  Iniciativa 2.3. Aprimorar a percepção de utilidade das informações dos serviços no portal único Gov.br e atingir, no mínimo, setenta e cinco por cento de avaliações positivas, até 2022.

- **Objetivo 3 - Canais e serviços digitais simples e intuitivos**

  Iniciativa 3.1. Estabelecer padrão mínimo de qualidade para serviços públicos digitais, até 2020;

  Iniciativa 3.2. Realizar, no mínimo, cem pesquisas de experiência com os usuários reais dos serviços públicos, até 2022.

- **Objetivo 4 - Acesso digital único aos serviços públicos**

  Iniciativa 4.1. Consolidar mil e quinhentos domínios do Governo federal no portal único Gov.br, até 2020;

  Iniciativa 4.2. Integrar todos os Estados à Rede Gov.br, até 2022;

  Iniciativa 4.3. Consolidar a oferta dos aplicativos móveis na conta única do Governo federal nas lojas, até 2020;

  Iniciativa 4.4. Ampliar a utilização do login único de acesso Gov.br para mil serviços públicos digitais, até 2022.

- **Objetivo 5 - Plataformas e ferramentas compartilhadas**

  Iniciativa 5.1. Implementar meios de pagamentos digitais para, no mínimo, trinta por cento dos serviços públicos digitais que envolvam cobrança, até 2022;

  Iniciativa 5.2. Disponibilizar plataforma de caixa postal digital do cidadão.

- **Objetivo 6 - Serviços públicos integrados**

  Iniciativa 6.1. Interoperar os sistemas do Governo federal, de forma que, no mínimo, novecentos serviços públicos contem com preenchimento automático de informações, até 2022;

  Iniciativa 6.2. Ampliar para vinte a quantidade de atributos no cadastro base do cidadão, até 2022;

  Iniciativa 6.3. Estabelecer quinze cadastros base de referência para interoperabilidade do Governo federal, até 2022;

  Iniciativa 6.4. Estabelecer barramento de interoperabilidade dos sistemas do Governo federal, até 2020, de forma a garantir que pessoas, organizações e sistemas computacionais compartilhem os dados.

- **Objetivo 7 - Políticas públicas baseadas em dados e evidências**

  Iniciativa 7.1. Produzir quarenta novos painéis gerenciais de avaliação e monitoramento de políticas públicas, até 2022;

  Iniciativa 7.2. Catalogar, no mínimo, as trezentas principais bases de dados do Governo Federal, até 2022;

  Iniciativa 7.3. Disponibilizar o mapa de empresas no Brasil, até 2020.

- **Objetivo 8 - Serviços públicos do futuro e tecnologias emergentes**

  Iniciativa 8.1. Desenvolver, no mínimo, seis projetos de pesquisa, desenvolvimento e inovação com parceiros do Governo federal, instituições de ensino superior, setor privado e terceiro setor, até 2022;

Iniciativa 8.2. Implementar recursos de inteligência artificial em, no mínimo, doze serviços públicos federais, até 2022;

Iniciativa 8.3. Disponibilizar, pelo menos, nove conjuntos de dados por meio de soluções de *blockchain* na administração pública federal, até 2022;

Iniciativa 8.4. Implementar recursos para criação de uma rede *blockchain* do Governo Federal interoperável, com uso de identificação confiável e de algoritmos seguros;

Iniciativa 8.5. Implantar um laboratório de experimentação de dados com tecnologias emergentes.

- **Objetivo 9 - Serviços preditivos e personalizados ao cidadão**

  Iniciativa 9.1. Implantar mecanismo de personalização da oferta de serviços públicos digitais, baseados no perfil do usuário, até 2022;

  Iniciativa 9.2. Ampliar a notificação ao cidadão em, no mínimo, vinte e cinco por cento dos serviços digitais.

- **Objetivo 10 - Implementação da Lei Geral de Proteção de Dados no âmbito do Governo federal**

  Iniciativa 10.1. Estabelecer método de adequação e conformidade dos órgãos com os requisitos da Lei Geral de Proteção de Dados, até 2020;

  Iniciativa 10.2. Estabelecer plataforma de gestão da privacidade e uso dos dados pessoais do cidadão, até 2020.

- **Objetivo 11 - Garantia da segurança das plataformas de governo digital e de missão crítica**

  Iniciativa 11.1. Garantir, no mínimo, noventa e nove por cento de disponibilidade das plataformas compartilhadas de governo digital, até 2022;

  Iniciativa 11.2. Monitorar, no mínimo, oitenta por cento dos riscos de segurança cibernética nas plataformas compartilhadas de governo digital;

  Iniciativa 11.3. Definir padrão mínimo de segurança cibernética a ser aplicado nos canais e serviços digitais.

- **Objetivo 12 - Identidade digital ao cidadão**

  Iniciativa 12.1. Prover dois milhões de validações biométricas mensais para serviços públicos federais, até o final de 2020;

  Iniciativa 12.2. Disponibilizar identidade digital ao cidadão, com expectativa de emissão de quarenta milhões, até 2022;

Iniciativa 12.3. Criar as condições para a expansão e para a redução dos custos dos certificados digitais para que custem, no máximo R$ 50,00 (cinquenta reais) por usuário anualmente, até 2022;

Iniciativa 12.4. Disponibilizar novos mecanismos de assinatura digital ao cidadão, até 2022;

Iniciativa 12.5. Incentivar o uso de assinaturas digitais com alto nível de segurança;

Iniciativa 12.6. Estabelecer critérios para adoção de certificado de atributos para simplificação dos processos de qualificação de indivíduo ou entidade;

Iniciativa 12.7. Promover a divulgação ampla de sistemas e aplicações para uso e verificação das políticas de assinatura com códigos abertos e interoperáveis.

- **Objetivo 13 - Reformulação dos canais de transparência e dados abertos**

Iniciativa 13.1. Integrar os portais de transparência, de dados abertos e de ouvidoria ao portal único Gov.br, até 2020;

Iniciativa 13.2. Ampliar a quantidade de bases de dados abertos, de forma a atingir 0,68 (sessenta e oito centésimos) pontos no critério de disponibilidade de dados do índice organizado pela Organização para a Cooperação e Desenvolvimento Econômico, até 2022;

Iniciativa 13.3. Melhorar a qualidade das bases de dados abertos, de forma a atingir 0,69 (sessenta e nove décimos) pontos no critério de acessibilidade de dados do índice organizado pela Organização para a Cooperação e Desenvolvimento Econômico, até 2022.

- **Objetivo 14 - Participação do cidadão na elaboração de políticas públicas**

Iniciativa 14.1. Firmar parcerias para a construção de aplicações de controle social, por meio de três *datathons* ou *hackathons*, até 2022;

Iniciativa 14.2. Aprimorar os meios de participação social e disponibilizar nova plataforma de participação, até 2021.

- **Objetivo 15 - Governo como plataforma para novos negócios**

Iniciativa 15.1. Disponibilizar, no mínimo, vinte novos serviços interoperáveis que interessem às empresas e às organizações, até 2022;

Iniciativa 15.2. Firmar parcerias com instituições representativas da indústria de tecnologia da informação, comunicação e de identificação digital, com reconhecida participação colaborativa.

- **Objetivo 16 - Otimização das infraestruturas de tecnologia da informação**

  Iniciativa 16.1. Realizar, no mínimo, seis compras centralizadas de bens e serviços comuns de tecnologia da informação e comunicação, até 2022;

  Iniciativa 16.2. Ampliar o compartilhamento de soluções de software estruturantes, totalizando um novo software por ano, até 2022;

  Iniciativa 16.3. Ofertar, no mínimo, quatro soluções de tecnologia da informação e comunicação por meio do *marketplace*, até 2022;

  Iniciativa 16.4. Otimizar a infraestrutura de, pelo menos, trinta *data centers* do Governo Federal, até 2022;

  Iniciativa 16.5. Migração de serviços de, pelo menos, trinta órgãos para a nuvem, até 2022;

  Iniciativa 16.6. Negociar acordos corporativos com os maiores fornecedores de tecnologia da informação e comunicação do governo, de forma a resultar na redução de, no mínimo, vinte por cento dos preços de lista, até 2022.

- **Objetivo 17 - O digital como fonte de recursos para políticas públicas essenciais**

  Iniciativa 17.1. Aprimorar a metodologia de medição da economia de recursos com a transformação digital, até 2020;

  Iniciativa 17.2. Disponibilizar painel com o total de economia de recursos auferida com a transformação digital, até 2020;

  Iniciativa 17.3. Estabelecer processo de reinvestimento da economia auferida com a transformação digital, em políticas públicas essenciais, até 2021.

- **Objetivo 18 - Equipes de governo com competências digitais**

  Iniciativa 18.1. Capacitar, no mínimo, dez mil profissionais das equipes do Governo federal em áreas do conhecimento essenciais para a transformação digital;

  Iniciativa 18.2. Difundir os princípios da transformação digital por meio de eventos e ações de comunicação, de forma a atingir, no mínimo, cinquenta mil pessoas, até 2022;

  Iniciativa 18.3. Ampliar a força de trabalho dedicada à transformação digital na administração pública federal, em dois mil profissionais, até 2022.

9. ATUALIZAÇÃO

9.1. Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser revisados anualmente, ou por deliberação do CGD.

9.2. O CGD formalizará a proposta de revisão da PoSIC por meio de instrumento legal, o qual deve ser aprovado pelo reitor da Unifesspa.

Modelo de referência: PoSIC do Ministério do Planejamento, Orçamento e Gestão – Portaria MP nº 27 de 3/02/2012 (DOU 06/02/2012)

REFERÊNCIAS LEGAIS E NORMATIVAS

I - DISPOSITIVOS LEGAIS DE CARÁTER FEDERAL, APLICÁVEIS À SEGURANÇA DA INFORMAÇÃO:

- Constituição Federal, art. 5º, inciso X. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.

- Constituição Federal, art. 5º, inciso XII. Sigilo dos dados telemáticos e das comunicações privadas.

- Constituição Federal, art. 5º, inciso XIV. Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.

- Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II. Disponibilidade das informações constantes nos órgãos públicos.

- Constituição Federal, art. 5º, inciso XXXIV. Disponibilidade das informações constantes nos órgãos públicos.

- Constituição Federal, art. 23, incisos III e IV. Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.

- Constituição Federal, art. 216, § 2º. Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.

- Constituição Federal, art. 37, caput. Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.

- Constituição Federal, art. 37, § 6º e Código Civil, art. 43. Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.

- Constituição Federal, art. 37, § 7º. Necessidade de regulamentação do acesso a informações privilegiadas.

- Consolidação das Leis do Trabalho - CLT, art. 482, alínea "g". Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).

- Código de Conduta da Alta Administração, art. 5º, § 4º. Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).

- Código de Conduta da Alta Administração, art.14, inciso II. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II. Proteção da integridade das informações públicas.

- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "l" do inciso XV da Seção II. Proteção da disponibilidade das informações públicas.

- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso X da Seção I. Proteção da disponibilidade das informações públicas.

- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso VII da Seção I. Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.

- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso IX da Seção I. Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.

- Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II. Disponibilidade das comunicações.

- Código de Propriedade Industrial, art. 75. Sigilo das patentes de interesse da defesa nacional.

- Código de Defesa do Consumidor, arts. 43 e 44. Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.

- Código Penal, art. 151. Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.

- Código Penal, art. 152. Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.

- Código Penal, art. 153. Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.

- Código Penal, art. 154. Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.

- Código Penal, art. 184, § 3º. Proteção da autenticidade.

- Código Penal, art. 297. Proteção da integridade e autenticidade dos documentos públicos.

- Código Penal, art. 298. Proteção da integridade e autenticidade dos documentos particulares.

- Código Penal, art. 305. Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.

- Código Penal, art. 307. Proteção da autenticidade.

- Código Penal, art. 313-A. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

- Código Penal, art. 313-B. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

- Código Penal, art. 314. Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.

- Código Penal, art. 325. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

- Código Processo Penal, art. 20. Proteção de informações sigilosas.

- Código Processo Penal, art. 207. Proteção do sigilo profissional.

- Código Processo Penal, art. 745. Proteção de informações sigilosas relacionadas ao condenado.

- Código Tributário Nacional, art. 198. Proteção do sigilo fiscal.

- Código de Processo Civil, art. 347, inciso II c/c art. 363, inciso IV. Proteção da privacidade de seus clientes.

- Código de Processo Civil, art. 406, inciso II c/c art. 414, § 2º. Proteção da privacidade de seus clientes.

- Instrução Normativa nº 4/2010 Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.

- Lei nº 6.538/1978, art. 41. Proteção da privacidade de correspondência.

- Lei nº 7.170/1983, art. 13. Proteção das informações sigilosas relacionadas à segurança nacional.

- Lei nº 7.232/1984, art. 2º, inciso VIII. Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.

- Lei nº 7.492/1986, art. 18. Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.

- Lei nº 8.027/1990, artigo 5º, inciso I. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

- Lei nº 8.027/1990, artigo 5º, parágrafo único, inciso V. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

- Lei nº 8.112/1990, art. 116, inciso VIII. Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.

- Lei nº 8.112/1990, art. 132, inciso IX. Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.

- Lei nº 8.137/1990, art. 3º, inciso I. Proteção da disponibilidade de informações para manutenção da ordem tributária.

- Lei nº 8.429/1992, art.11, incisos III, IV e VII. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.

- Lei nº 8.429/1992, art. 13. Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.

- Lei nº 8.443/1992, art. 86, inciso IV. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

- Lei Complementar nº 75/1993, art. 8º incisos II e VIII, §§ 1º e 2º. Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

- Lei nº 8.625/1993, art. 26, inciso I, alínea "b" e inciso II. Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

- Lei nº 8.906/1994, art. 7º, inciso XIX. Proteção da privacidade do cliente do advogado.

- Lei nº 9.100/1995, art. 67, incisos VII e VIII. Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.

- Lei nº 9.279/1996, art. 195, inciso XI. Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.

- Lei nº 9.296/1996, art. 10. Sigilo dos dados e das comunicações privadas.

- Lei nº 9.472/1997, art. 3º, inciso V. Sigilo das comunicações.

- Lei nº 9.472/1997, art. 3º, inciso VI. Proteção de informações pessoais de caráter sigiloso.

- Lei nº 9.472/1997, art. 3º, inciso IX. Proteção de informações pessoais de caráter sigiloso.

- Lei nº 9.504/1997, art. 72. Proteção da integridade das informações de caráter eleitoral e dos equipamentos.

- Lei nº 9.605/1998, art. 62. Disponibilidade e integridade de dados e informações.

- Lei nº 10.683/2003, art. 6º. Todos os aspectos da segurança da informação.

- Lei nº 10.703/2003, arts. 1º, 2º e 3º. Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.

- Decreto nº 4.801/2003, art. 1º, inciso X. Todos os aspectos da segurança da informação.

- Decreto nº 5.483/2005, arts. 3º e 11. Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.

- Decreto nº 5.687/2006, arts.10 e 13 do Anexo. Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.

- Decreto nº 6.029/2007, inciso II do art. 1º. Disponibilidade das informações constantes nos registros públicos.

- Decreto nº 6.029/2007, art. 10. Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.

- Decreto nº 6.029/2007, art. 13. Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.

- Decreto nº 6.029/2007, art. 22. Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

II - LEGISLAÇÃO ESPECÍFICA DE CARÁTER FEDERAL RELACIONADA À SEGURANÇA DA INFORMAÇÃO:

- Lei nº 7.232/1984 Dispõe sobre a Política Nacional de Informática, e dá outras providências.

- Lei nº 8.248/1991 Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.

- Lei nº 9.296/1996 Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.

- Lei nº 9.472/1997 Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.

- Lei nº 9.507/1997 Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

- Lei nº 9.609/1998 Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

- Lei nº 9.883/1999 Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.

- Lei nº 8.159/1991 Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.

- Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

- Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

- Lei nº 10.973, de 02 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.

- Lei nº 11.111, de 05 de maio de 2005. Regula o direito à informação e ao acesso aos registros públicos.

- Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 ¿ Código de Processo Civil; e dá outras providências.

- Decreto nº 2.295, de 04 de agosto de 1997. Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.

- Decreto nº 2.556, de 20 de abril de 1998. Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

- Decreto nº 3.294, de 15 de dezembro de 1999. Institui o Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.

- Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

- Decreto de 18 de outubro de 2000. Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.

- Decreto nº 3.714, de 03 de janeiro de 2001. Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto nº 2.954, de 29 de janeiro de 1999, e dá outras providências.

- Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

- Decreto nº 4.073, de 03 de janeiro de 2002. Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

- Decreto nº 4.376, de 13 de setembro de 2002. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.

- Decreto nº 4.522, de 17 de dezembro de 2002. Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.

- Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

- Decreto nº 4.689, de 07 de maio de 2003. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências.

- Decreto nº 4.829, de 03 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.

- Decreto de 29 de outubro de 2003. Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências.

- Decreto nº 5.301, de 09 de dezembro de 2004. Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.

- Decreto nº 5.450, de 31 de maio de 2005. Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.

- Decreto nº 5.563, de 11 de outubro de 2005. Regulamenta a Lei nº 10.973, de dezembro de 2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências.

- Decreto nº 5.584, de 18 de novembro de 2005. Dispõe sobre o recolhimento ao Arquivo Nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN.

- Decreto nº 5.772, de 08 de maio de 2006, art. 8º. Institui na estrutura regimental do Gabinete de Segurança Institucional da Presidência da República o Departamento de Segurança da Informação e Comunicações com diversas atribuições na área de segurança da informação e comunicações.

- Decreto nº 6.605, de 14 de outubro de 2008. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.

- Instrução Normativa nº 1 do GSI, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

- Resolução nº 58 do INPI, de 14 de julho de 1998. Estabelece normas e procedimentos relativos ao registro de programas de computador.

- Resolução nº 59 do INPI, de 14 de julho de 1998. Estabelece os valores das retribuições pelos serviços de registro de programas de computador.

- Resolução nº 338 do STF, de 11 de abril de 2007. Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF.

- Resolução nº 140 do TST, de 13 de setembro de 2007. Regulamenta, no âmbito da Justiça do Trabalho, a Lei nº 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.

- Resolução nº 22.718/2008 do TSE, arts. 18 e 19. Regula a propaganda eleitoral na internet em campanha nas eleições de 2008.

III - Normas técnicas relacionadas à segurança da informação:

- ISO/IEC TR 13335-3:1998. Esta norma fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.

- ISO/IEC GUIDE 51:1999. Esta norma fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).

- ISO/IEC GUIDE 73:2002. Esta norma fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.

- ABNT NBR ISO IEC 17799: 2005. Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.

- ABNT NBR ISO/IEC 27001:2005. Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.